Information Security Policy *detailing Flempton Golf Club's (FGC) approach to information security, the technical and organisational measures that will be implemented and the roles and responsibilities officers and staff have in relation to keeping information secure.*

The objective of FGC's Information Security Policy is to ensure that all information and information systems, on which the club depends, are adequately protected. Achieving this largely depends on club officials working diligently in accordance with policy guidelines.

The Information Security Policy sets out requirements and recommendations, relating to how:
Confidential information must be protected from unauthorised access.
The integrity of information and information systems must be protected.
Appropriate measures must be taken to manage risks to the availability of information.
The Club must ensure compliance with laws and the terms of contracts.

Compliance:
It is the responsibility of each individual to ensure that they do not break the law or cause a breach in The Club IT system or data protection policy.
Officers that may use the information system, or handle club data must be explicitly informed and confirm acceptance of the club policy towards use of The Clubs personal data and IT systems.

Outsourcing and Third Party Access
Outsourcing IT arrangements should be part of a formal contract
External organisations accessing FGC information system must be risk-managed and where appropriate part of a formal agreement.
A risk assessment should be made and appropriate controls used (supervised) where contractors or other external parties have or are given physical access to areas where confidential information is stored or processed.

Personnel
Officers must agree to abide by the information security policies as a condition of using any FLG system or handling FGC data. All users must be identified.

Operations
Access to the club IT systems must be restricted to officers involved in administering the system, password protected and access documented. Security incidents and software faults must be reported.

Information Handling
Individuals must comply with any legal compliance requirements or implicit expectations when handling information.
Responsibility for managing information assets must be assigned.
Appropriate backup arrangements must be implemented.
Confidential documents must be shredded.
Electronic data must be securely deleted (simple file deletion is often inadequate)

Use of Computer
Any device connected to a network, must meet the currently required hardware and software standards.
It is unacceptable to use the IT facilities for illegal activities; creation or transmission of any offensive, obscene or indecent images, data or other material; create or transmit material intent to cause annoyance or needless anxiety, defraud, or violate the privacy of others. All incidents should be reported.

Software Management
Software must be licenced, unlicensed software should be licenced or uninstalled.
Operating systems should be maintained.
Software containing malware of any type should be removed or the maleware deactivated.